

Client Certificate Import Manual

Rev. 1.4

【INDEX】

This is a user manual for importing the client certificate for VPN under the following terminal environments.

- [Windows Vista / Windows 7](#) [P 2](#)
- [Windows 8 / Windows8.1](#) [P 8](#)
- [Mac OSX 10.7 / 10.8 /10.9 / 10.10](#) [P 14](#)

If you want to remove the imported certificate, check the following.

- [Windows Vista / Windows 7](#) [P 6](#)
- [Windows 8 / Windows8.1](#) [P 12](#)
- [Mac OSX 10.7 / 10.8 /10.9 / 10.10](#) [P 16](#)

※ This user manual must be executed by users with **administrative authority**.

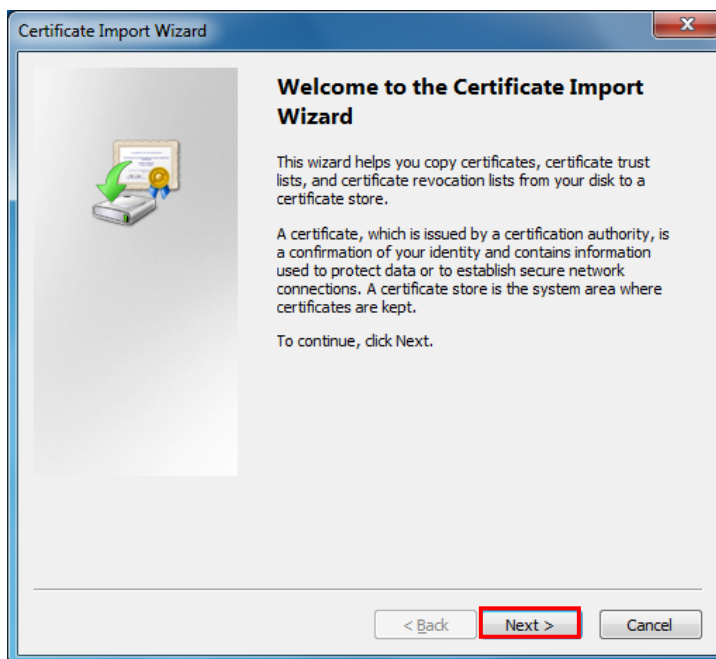
【Windows Vista / Windows 7】

◆Client Certificate Import Manual◆

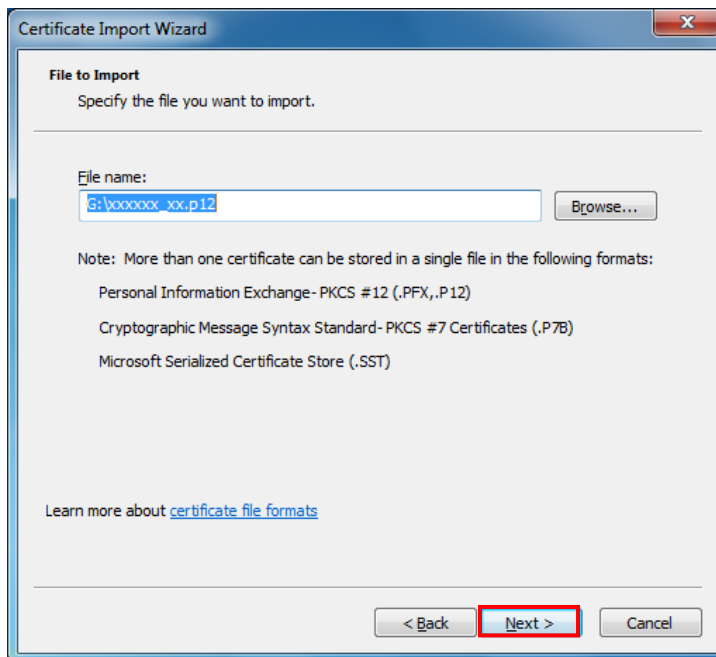
Double click the certificate file distributed by the administrator.



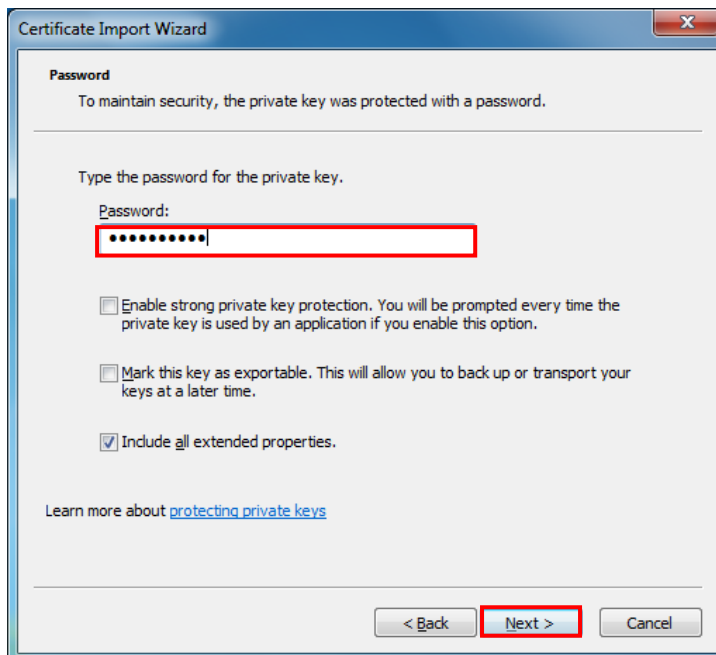
The **Certificate Import Wizard** will appear. Click **Next**.



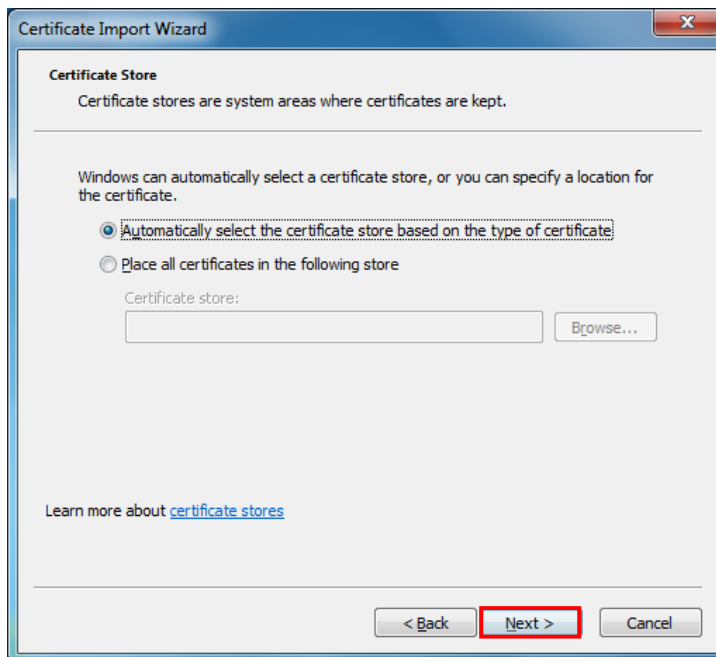
The certificate will be stored in the location specified. Click **Next**.



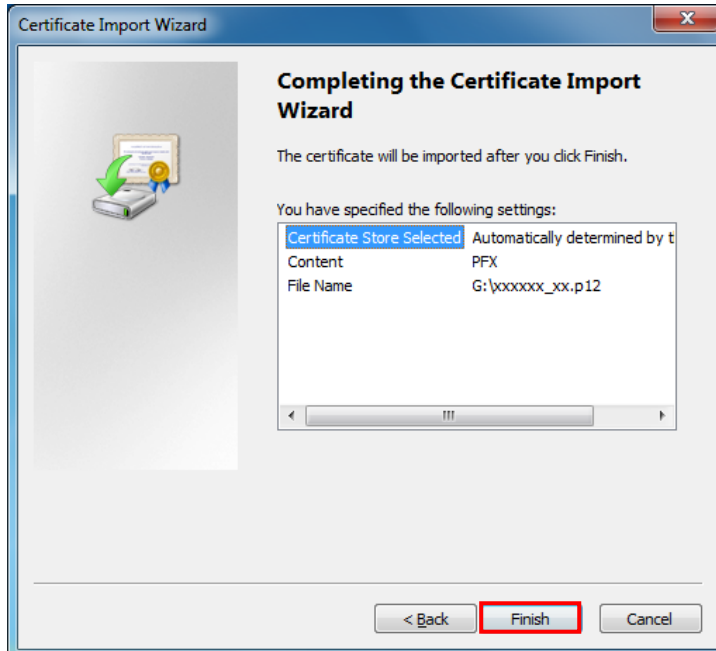
Enter the password you received with the certificate and click **Next**.



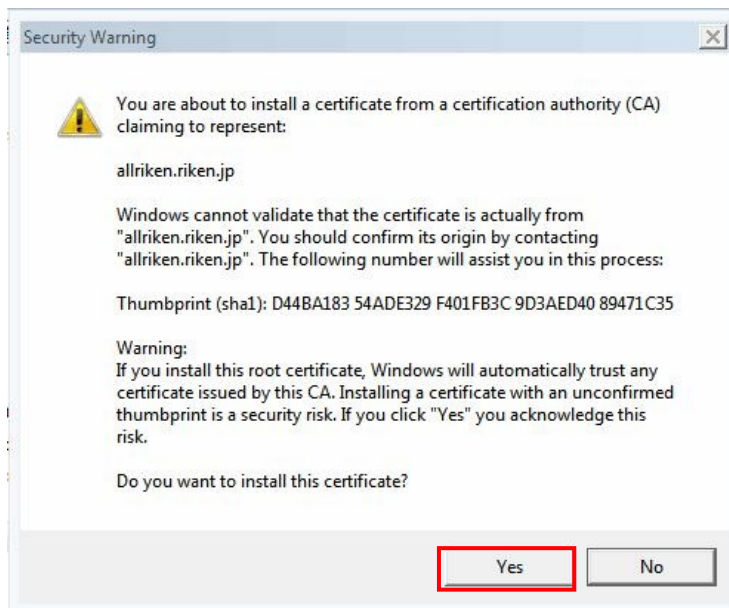
Automatically select the certificate store... should be selected. Click **Next**.



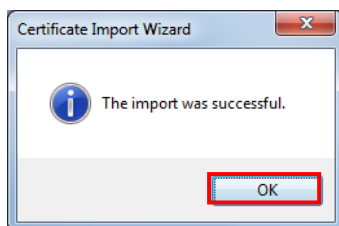
Finish the import wizard by clicking **Finish**.



A **security warning** will appear. Click **Yes**.



The certificate has been imported. Click **OK**.

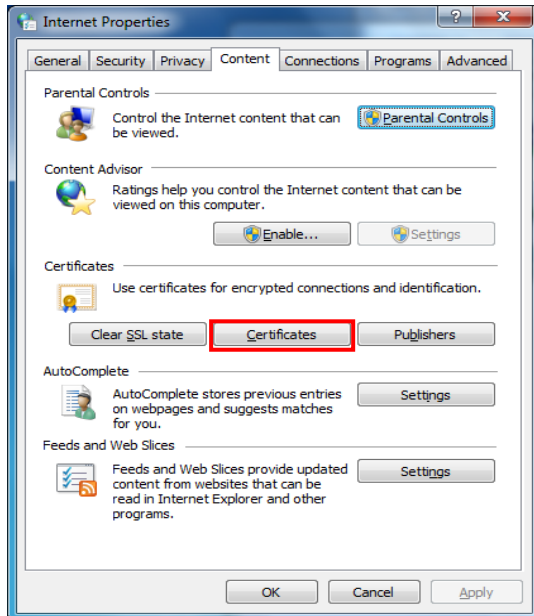


◆Client Certificate Delete Manual◆

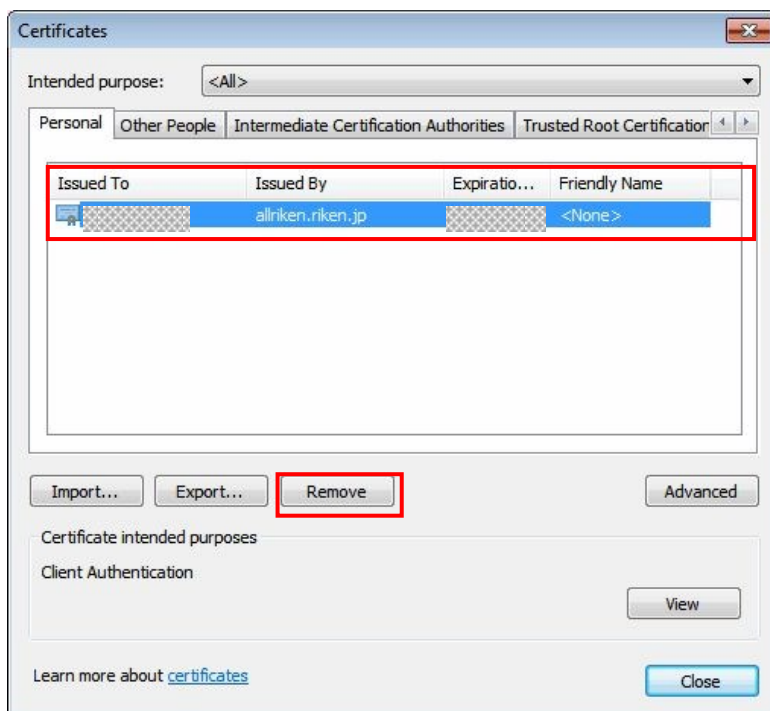
Open Internet Options.

Click on **Start**->**Control Panel**->**Network and Internet** and click **Internet Options**.

Select the **Content** tab and click **Certificates**.

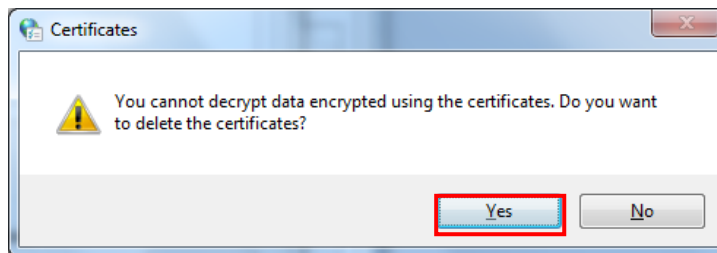


Select the certificate issued by **allriken.riken.jp** in the **Personal** tab, and click **Remove**.



Windows Vista / Windows 7

Click **Yes**.



【Windows 8 / Windows 8.1】

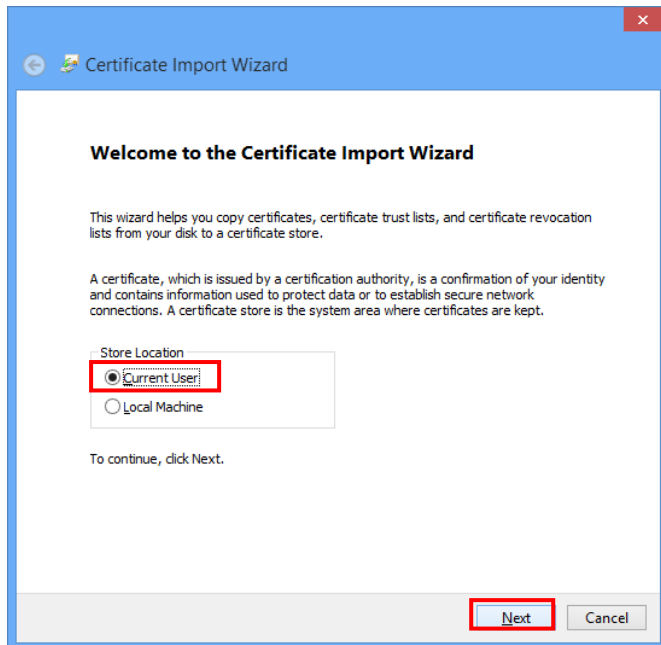
◆Client Certificate Import Manual◆

Double click the certificate file distributed by the administrator.



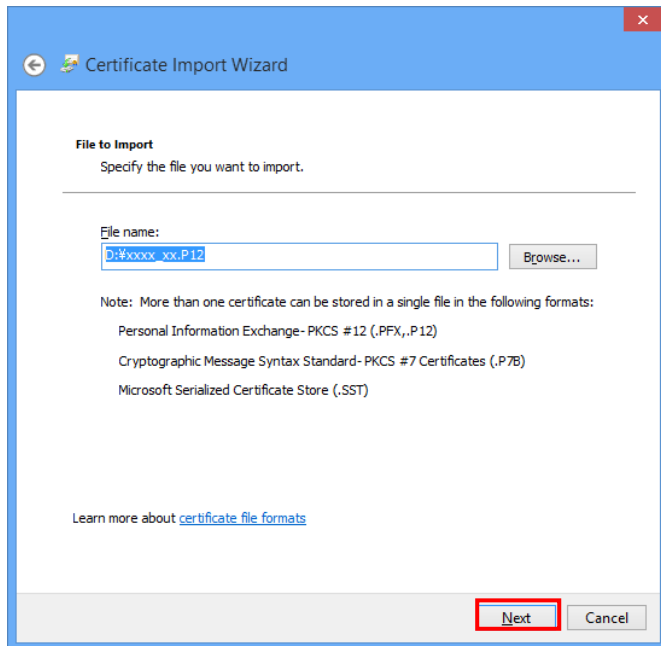
The **Certificate Import Wizard** will appear.

Current User should be selected. Click **Next**.



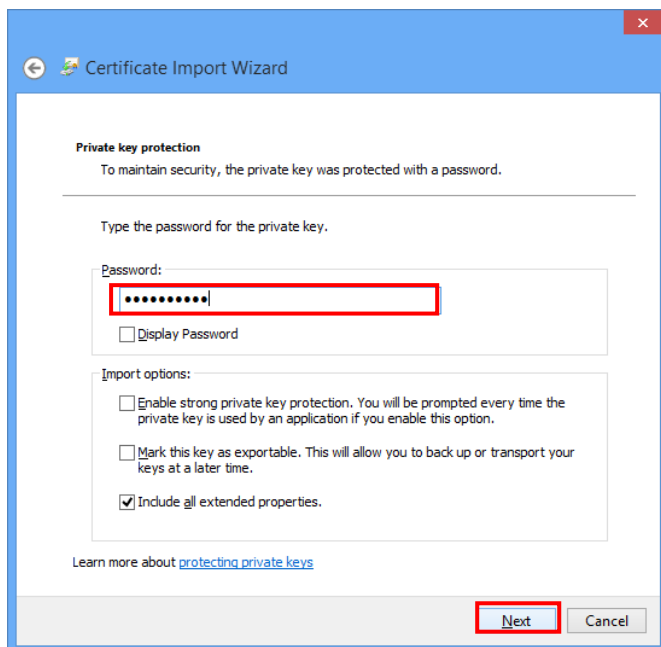
Windows 8 / Windows 8.1

The certificate will be stored in the location specified. Click **Next**.



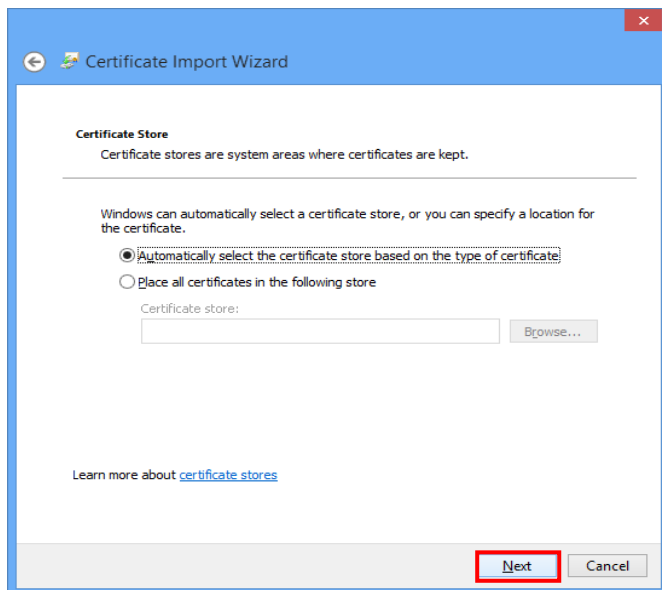
The screenshot shows the 'File to Import' step of the Certificate Import Wizard. The title bar reads 'Certificate Import Wizard'. The main heading is 'File to Import' with the instruction 'Specify the file you want to import.' Below this is a text box for 'File name:' containing 'D:\xxxx_xx.P12' and a 'Browse...' button. A note states: 'Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange- PKCS #12 (.PFX,.P12), Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B), Microsoft Serialized Certificate Store (.SST)'. A link 'Learn more about certificate file formats' is at the bottom left. At the bottom right, the 'Next' button is highlighted with a red rectangle, and a 'Cancel' button is next to it.

Enter the password you received with the certificate and click **Next**.

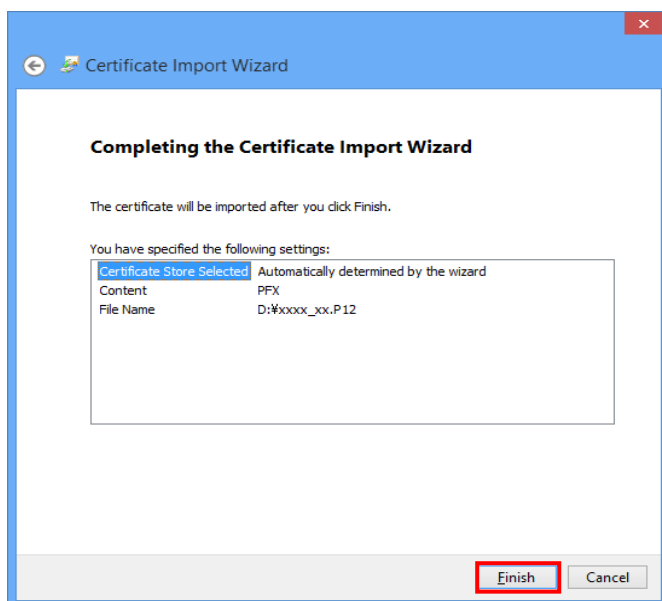


The screenshot shows the 'Private key protection' step of the Certificate Import Wizard. The title bar reads 'Certificate Import Wizard'. The main heading is 'Private key protection' with the instruction 'To maintain security, the private key was protected with a password.' Below this is the text 'Type the password for the private key.' and a 'Password:' label. A text box for the password is highlighted with a red rectangle and contains ten dots. Below the password box is a checkbox labeled 'Display Password'. Under the heading 'Import options:', there are three checkboxes: 'Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.' (unchecked), 'Mark this key as exportable. This will allow you to back up or transport your keys at a later time.' (unchecked), and 'Include all extended properties.' (checked). A link 'Learn more about protecting private keys' is at the bottom left. At the bottom right, the 'Next' button is highlighted with a red rectangle, and a 'Cancel' button is next to it.

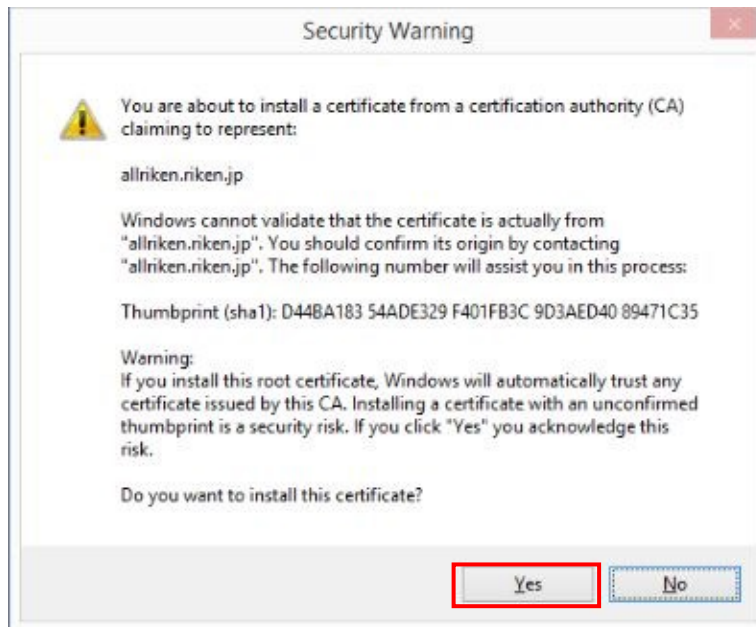
Automatically select the certificate store... should be selected. Click **Next**.



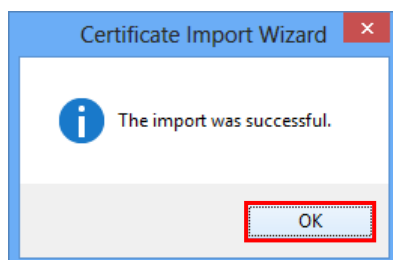
Finish the import wizard by clicking **Finish**.



A **security warning** will appear. Click **Yes**.



The certificate has been imported. Click **OK**.

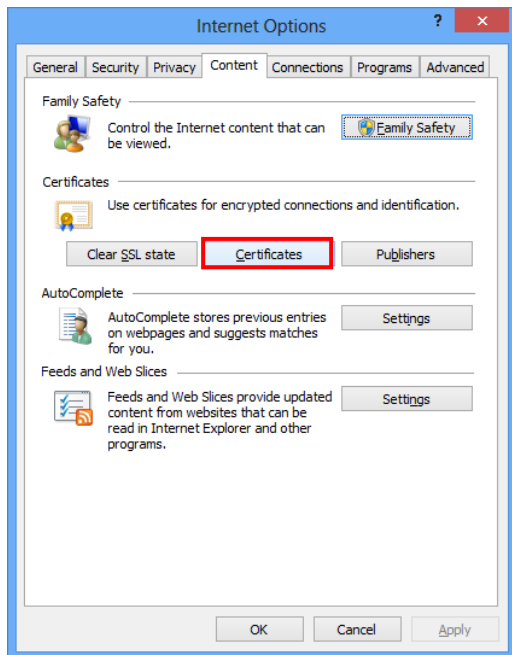


◆Client Certificate Delete Manual◆

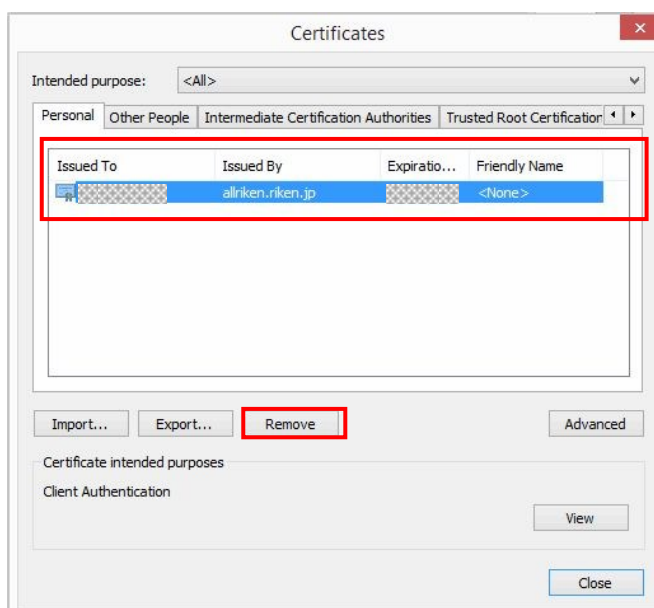
Open Internet Options.

Go to **Settings**→**Control Panel**→**Network and Internet Connections** and click **Internet Options**.

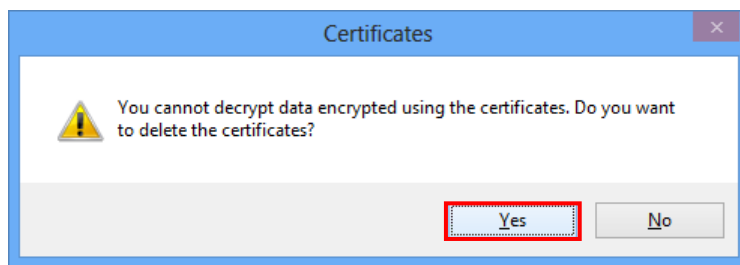
Select the **Content** tab and click **Certificates**.



Select the certificate issued by **allriken.riken.jp** in the **Personal** tab, and click **Remove**.



Click **Yes**.



【Mac OSX 10.7 / 10.8 / 10.9 / 10.10】

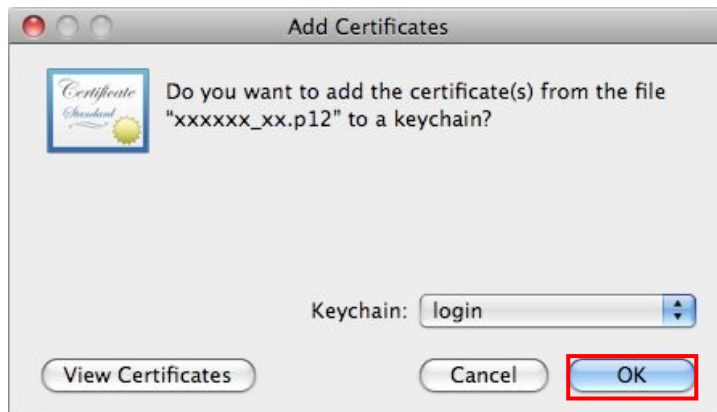
◆Client Certificate Import Manual◆

Double click the certificate file (extension.P12) distributed by the administrator.



Add Certificates will appear. Make sure login is selected in **Keychain** and click **OK**.

※If you are using Mac OSX 10.10 or later, go on to the next procedure.

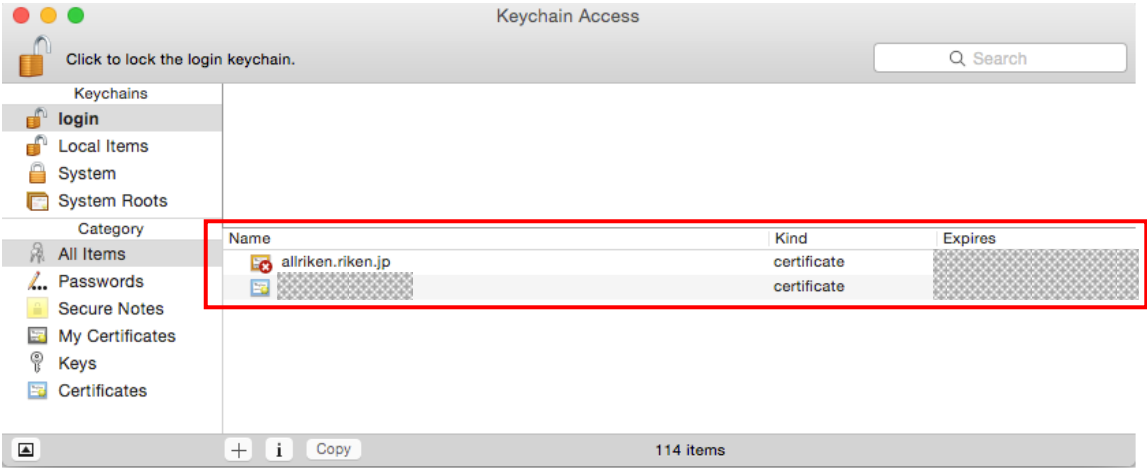


Enter the password you received with the certificate and click **OK**.

It's complete.



Go to **Finder->Applications->Utilities** and open **Keychain Access**.
Two certificates under the name **Login ID** and **allriken.riken.jp** should be created.
Then importing the Client Certificate is completed.



◆Client Certificate Delete Manual◆

Open **Keychain Access**.

Go to **Finder->Applications->Utilities** and open **Keychain Access**.

Select the certificates **RIKEN ID** and **allriken.riken.jp** and click **Delete**.

